Is there anything else like the complex numbers?

A. Eremenko

August 3, 2021

1. The following question is frequently asked in my office hours: *What is so special about complex numbers? Can one define a multiplication of vectors in* $\mathbf{R}^n$ *so that a field is obtained ?*

I recall what is a field. It is a set with two operations, addition and multiplication, which have the "usual properties", that is

- both operations are commutative and associative,
- there are elements 0 such that $x + 0 = x$ for all x, and 1 such that $1x = x$ for all x, and $0 \neq 1$.
- both operations are invertible: for every x there is y such that $x+y = 0$ and for every $x \neq 0$ there is w such that $xw = 1$.
- distributive law holds: $x(y + z) = xy + xz$.

Examples of fields are: rational numbers $\mathbf{Q}$, real numbers $\mathbf{R}$, complex numbers $\mathbf{C}$.

There are many more examples, the simplest is the field which consists of only two elements, 0 and 1. In this field $1 + 1 = 0$, and $1 \times 1 = 1$. The rest of the multiplication and addition tables is filled so that the definition of the field is satisfied, that is

$$0 + 0 = 0, \quad 1 + 0 = 0 + 1 = 1, \quad 0 \times 0 = 0, \quad 1 \times 0 = 0 \times 1 = 0.$$

You can easily verify that with these definitions, all properties of the field stated above are satisfied.

Other examples of fields are *rational functions* with rational or real or complex coefficients, with usual operations of addition and multiplication.

Now, let us return to the original question: consider $\mathbf{R}^n$, the set of column vectors with real entries and usual operations of addition and multiplication of a vector by a real number. Can one define a product of such vectors, so that the result is a filed ?

It turns out that one can do this *only* in two cases: $n = 1$ (the usual multiplication of real numbers) and $n = 2$ (the complex multiplication). This remarkable fact follows from a theorem of Frobenius stated below.

This fact shows that $\mathbf{R}$ and $\mathbf{C}$ are quite exceptional.

You probably know the so-called vector product of vectors in $\mathbf{R}^3$. This product does not turn $\mathbf{R}^3$ into a field, because it is not commutative and not associative.

One can ask a more general question, whether we can define a product in $\mathbf{R}^n$ which has all properties listed above, except one: commutativity. The answer is given by the Frobenius theorem: *An associative, distributive product on $\mathbf{R}^n$, such that all non-zero vectors have multiplicative inverses exists only when $n = 1, 2$ or 4. When $n = 1$ and $n = 2$ these are real and complex numbers, when $n = 4$ these are so-called* quaternions.

In particular, there is no distributive, associative product on $\mathbf{R}^3$ such that every non-zero vector has a multiplicative inverse.

The proof of the Frobenius theorem uses only linear algebra, and I can recommend two places where you can read it. One is Pontryagin's book [1], chapter 4, section 26 B; this is an advanced book. Another is the little book [2] which has no prerequisites, and explains everything (including linear algebra) from the beginning. This book is aimed at high school students and undergraduates.

2. There is another explanation why complex numbers (and real numbers) are very special, unique objects in Mathematics. It is the equality $|z_1 z_2| = |z_1||z_2|$. Let us write it in an expanded form, with $z_1 = a + bi$ and $z_2 = c + di$. Then $z_1 z_2 = (ac - bd) + (ad + bc)i$. Let us take squares of absolute values:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \tag{1}$$

In other words, *Product of sums of two squares is again is a sum of two squares.* Of course, every positive number is a sum of two squares of positive numbers (in infinitely many ways). But the identity also implies that product of sums of two squares of integers is again a sum of two squares of integers, which is not so trivial. And integers here can be replaced by anything for which sums and products are defined and satisfy the usual rules, for example by polynomials, rational functions etc. Relation (1) is just a formal algebraic identity.

The question arises whether there are similar identities with sums of n squares. Is the product of two sums of n squares always a sum of n squares? It turns out that this is so only for $n = 1, 2, 4$ and 8. This is called a theorem of Hurwitz.

The identity for $n = 1$ and $n = 2$ comes from multiplication of real and complex numbers, for $n = 4$, an example of such identity comes from multiplication of quaternions, and for $n = 8$ from multiplication of the so-called *octaves* of Cayley. Multiplication law of octaves (8-vectors) is distributive, but neither commutative nor associative, and every non-zero octave has a multiplicative inverse.

Another statement of the Hurwitz theorem is that multiplication of real numbers, complex numbers, quaternions and octaves are the only possible distributive multiplication laws with a unit in R^n, for which it is possible to define a dot (scalar) product, such that the length of the product equals the product of the lengths.

An elementary proof of Hurwitz's theorem can be also found in the same book [2].

References

[1] L. Pontryagin, Topological groups, Gordon and breach, NY, 1966.

[2] I. Kantor and A. Solodovnikov, Hypercomplex numbers, Springer, NY, 1989.